# Instituto Tecnológico y de Estudios Superiores de Occidente

Reconocimiento de validez oficial de estudios de nivel superior según acuerdo secretarial 15018, publicado en el Diario Oficial de la Federación del 29 de noviembre de 1976.

## Departamento de Electrónica, Sistemas e Informática

## Especialidad en Sistemas Embebidos


# System of data recollection, analysis and transfer by NFC for transport systems

---

**TRABAJO RECEPCIONAL** para obtener el **GRADO** de
**ESPECIALISTA EN SISTEMAS EMBEBIDOS**

Presentan: **BRANDON MIGUEL GONZÁLEZ LEYCEGUI, IVÁN [illegible]NIEL MAGDALENO CASILLAS, ALVARO BENJAMIN PULIDO BERNAL**

Director **MSC LUIS ENRIQUE GARABITO SIORDIA**

Tlaquepaque, Jalisco. julio de 2019.

# Aknowledgements

The authors would like to thank to our project advisor MSc Luis Enrique Garabito Siordia for his continuous support, availability and suggestions during the development of this research.

To Ph.D Lorena Michele Brennan Bourdon for her guidance during the writing process of this document.

To the Consejo Nacional de Ciencia y Tecnología (CONACYT) for the support and the Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO) for trusting and providing us with the necessary equipment through the development of the research.

# Abstract

*This paper shows the development and test of a prototype that collects and analyzes data of cycling trips, such as position, distance, speed, and travel time. This device was made to provide an extra security layer to the data transfer in embedded systems. The raw information that is produced by the project described in this paper is highly valued, so there is a need to record and transfer data in a secure way between electronic devices. The solution proposed in this project was based on the Near Field Communication (NFC) protocol to make the communication stage from an Electronic Control Unit to NFC tags, and then, the information stored in the tags can be read from smartphones that have an NFC module inside them. The data was generated from a Global Position System (GPS) module and antenna using the Haversine formula to calculate the distance between two geographical points, this considering the earth as a sphere to minimize the error produced taking the earth as a plane surface. A functional device that includes extra security of the data transfer in cycling trips, through NFC technology was successfully developed, however, future implementations can be extrapolated to other areas, such as the transportation sector.*

# Introduction

NFC is a standard technology that allows wireless data transmission between two devices over a short distance [1]. It operates under the concept of "touch and connect", in other words, it is required to keep both devices in proximity in order to begin the communication. A key aspect of the success of this technology is its accessibility, simplicity, and implementation in the smartphone market. These advantages allow developers to create a wide variety of applications, including contact sharing, retail store price tags, home door unlocking, smart device wireless charging [2], automotive implementations as interactions between the owner and the car, information retrieval, and the car key with NFC interface [3], among others. On the other hand, for the general public, NFC is currently available only in new and high-end devices.

In cycling and public transportation, the need to record data, such as position, distance, speed, and travel time is crucial to analyze the journey. The raw information that is produced is highly valued, and stored on devices that generate it, but it is always necessary to send this data to a destination for analysis. For this reason, a reliable transfer data method is necessary to satisfy this need. Nowadays, NFC technology is available to users through its high-end devices, this allows the transfer of sensitive information transfers through the encrypted authentication offered by Near Field Communication, such as payments or bank transfers [4]. By applying this technology, it is possible to solve the need for security in the transfer of information related to transportation.

NFC devices mainly fall in 2 functional categories: active and passive. Active devices accommodate a power source while passive devices do not. As a result, active devices have the capability of providing power to passive devices via Radio Frequency (RF) fields. A common passive NFC device is the NFC Tag, which can be used to store data, for instance, internet Unique Resource Locator (URL), text data, contact information, and so forth. One common use is to save data from travel in competitive cycling racing. Data recollection from cycling is a problem that is currently studied, previous approaches have used smartphones [5], IMU (Inertial Measure Unit) [6] and monocular cameras [7]. The secure transfer of the data is a key attack vector that could be minimized with NFC technology. Various studies have assessed the efficacy of the use of the NFC

technology emphasizing on how secure is to apply it and to control the data exchange [8], using tags as a mean of authentication to increase the security of the system [9].

Therefore, in order to ensure a safe transfer system of information, a device was adapted to a bicycle to help the user record data of the journey by recollecting information from a GPS (Global Position System). This device is capable of authenticating tags to help the owner keep travel information safe and most importantly, secure the vehicle with an electromechanical lock. In addition, a Light-Emitting Diode (LED) matrix display provides a visual aid to the user to assist during different situations, for instance, when a tag is denied or approved or when the GPS signal is inadequate or when the journey ends, by lighting a figure in the LED matrix.

The travel data recollection and transfer from the bicycle to an external medium is an opportunity for the development of safe data transmission using the NFC protocol [10] because of the security it offers and the simplicity in its use. This device consists of an NFC module, a GPS module, a LED matrix and a development board.

The development board selected for the proof of concept was the FRDM-K64F: Freedom Development Platform for Kinetis from NXP. For NFC communications, the OM23221ARD board from NXP was used, as it is compatible with our development board. Also, a Real Time Operating System (RTOS) was installed and configured to run the system's custom software.

# 1. Methodology

## 1.1. Secure data transfer by Near Field Communication

This project focuses on the development on the data recollection of the different sensors connected to the system and the secure data transfer. In order to receive data in a legible, effective, and simple manner from the NFC module or device, an NFC tag with the form of a sticker, was used [11] . The NFC module sends the information to the tag using the standard NFC Data Exchange Format (NDEF). These values represent the data recollected during the journey [12].

Before the process begins, the device authenticates the tag with its unique ID while it is near the NFC module. The authentication process within the device works by reading a previously saved tag ID from the flash memory and the ID from the received tag. Thereby, the first time the tag is near the device, if the ID of the tag matches the ID saved in the flash memory, access to the information will be granted. In addition, the device will open the lock for the bicycle user in order to move the vehicle and initiate the journey. On the other hand, if the set of values does not match, the access to the data is denied, the lock remains closed, and the start of the trip is not set. To stop the journey, the authorized tag must be scanned. As a result, the device will stop recollecting data, then, it will send the processed GPS data to the tag and prepare for a new journey. The modules are communicated as in Fig.1.

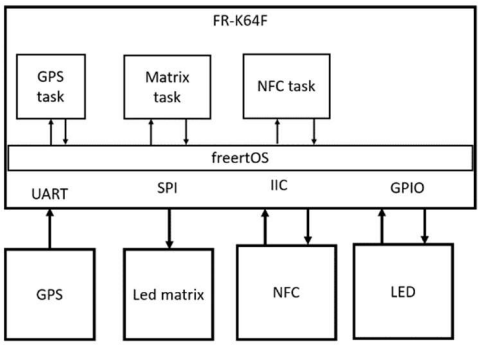


Figure 1-1 Communication module diagram.

The characteristics of the tags used for development and testing in this project are shown in the Table I. These tags have a maximum memory capacity of 144 bytes, this limits the amount of information transferred to the internal memory of the tags.

TABLE I
TAG CHARACTERISTICS

| | Description |
|---|---|
| Chip | NXP NTAG213 |
| Memory size | 180 bytes |
| Usable memory size | 144 bytes |
| Standard | ISO 14443 A |
| Frequency work | 13.56 MHz |
| RF distance | 1 to 5 cm |
| Data retention time | More than 10 years |

## 1.2. Analysis of the Recommended Minimum Data of GPS (RMC data frame)

The data recollection is performed through the GPS antenna, which sends the data using the National Marine Electronics Association (NMEA) standard. For analysis, the Recommended Minimum sentence C (RMC) frame is read, which contains useful information, such as latitude, longitude, time, and velocity, among others. These data are then used to calculate the average speed, total travel time, total distance traveled, including the start and finish position. The RMC frame was selected as it contains only the minimum information required for satellite navigation, which is enough data for the calculations. The communication between the GPS antenna and the main device is done via the Universal Asynchronous Receiver-Transmitter (UART) protocol as it is commonly implemented in almost any microcontroller device, due to its simplicity and low resources requirement.

Data incoming to the microcontroller unit (MCU) from the GPS module is stored and processed within a time period of less than a second. This feature helps minimize the error that occurs when measuring large distances between two geographic points. To calculate the distance between geographic coordinates, the Haversine formula (1-1) is used, which considers the curvature of the earth as a sphere, therefore, it produces a more accurate measurement of the

distance that do not consider the earth surface as curve [12]. Using a short sampling period of geographical points, it is not necessary to consider the earth as an ellipsoid; the difference is only reflected between the ellipsoid and the sphere over long distances.

Haversine formula:

$$D = 2 * R * \sin^{-1}\sqrt{A + B} \tag{1-1}$$

Where A means:

$$A = \sin^2\left(\frac{Lat_n - Lat_{n-1}}{2}\right) \tag{1-2}$$

And B is represented with formula:

$$B = \cos(Lat_{n-1}) * \cos(Lat_n) * \sin^2\left(\frac{Long_n - Long_{n-1}}{2}\right) \tag{1-3}$$

Where,

D = distance between two geographic coordinates.

R = radius of Earth (6372.795477 Km).

$Lat_n$ = latitude of last point in radians.

$Lat_{n-1}$ = latitude of previous point in radians.

$Long_n$ = longitude of last point in radians.

$Long_{n-1}$ = longitude of previous point in radians.

The GPS data is processed as it is shown in the next flow chart Fig. 1-2; this algorithm is executed depending on the scheduler of the real time operating system used in this project, FreeRTOS. Using a RTOS middleware helps manage the tasks in the application, included the GPS task, reserving the correct memory stack that will be used in run time, and controlling the execution times of each task.

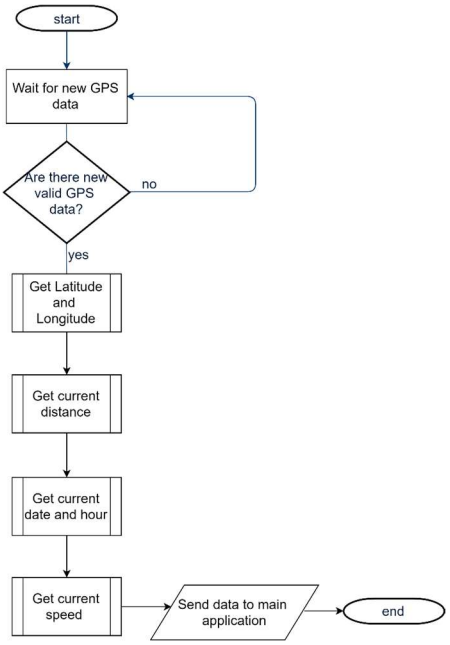


Figure 1-2 GPS data processing flow chart

## 1.3. LED Matrix

The LED matrix is a peripheral composed of the MAX7219 Integrated Circuit (IC) and an array of 64 LEDs arranged in an 8x8 pattern. This peripheral receives pre-defined images via Serial Peripheral Interface (SPI) and shows them on the display until a new image is received. The images were predefined during the design phase to be as simple as possible and to represent the 5 most important case scenarios: waiting for the GPS signal, end of trip and transfer data complete, lock closed, start of trip, and internal errors; the images selected include an hourglass, check mark symbol, lock close, lock open, and X mark symbol. For example, if the NFC module stops responding, a message is queued with the error scenario and the image of the “X” mark is sent via SPI to the external peripheral. More scenarios can be seen in Fig. 1-3.

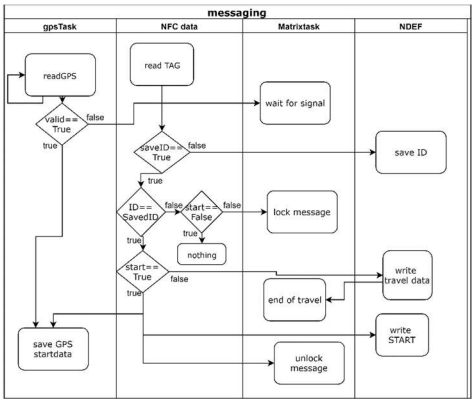


Figure 1-3 Messages sent in a standard travel

The device was able to obtain the ID from tags presented and start the analysis process, this process successfully compare the ID of the tag obtained with the ID stored in the flash memory in the device, when the ID matched it gave the user access to the information and opened the lock, when did not matched the information was deny it and maintained the lock closed. The ID stored in the flash memory allowed to maintain it in case of power loss or shutdown of the device, which permitted to continue with the validation of the tags to provide only the information to the ID stored in the flash memory and for the future journeys.

# 2. Results

The device was able to obtain the ID from tags presented and start the analysis process, this process successfully compare the ID of the tag obtained with the ID stored in the flash memory in the device, when the ID matched it gave the user access to the information and opened the lock, when did not matched the information was deny it and maintained the lock closed. The ID stored in the flash memory allowed to maintain it in case of power loss or shutdown of the device, which permitted to continue with the validation of the tags to provide only the information to the ID stored in the flash memory for future journeys.

The data from the travel was written in ASCII format and could be read as a text file as shown in Fig. 2-1. because of the memory size of the tag (142 bytes) we only printed the minimum information necessary, including the time, geolocation from the start and end of the travel, and the speed. Also, the decimals were truncated in the printed data to make the writing easier through a standard message size.

```
# NFC data set information:
NDEF message containing 1 record
Current message size: 142 bytes
Maximum message size: 142 bytes
NFC data set access: Read & Write
# Record #1: Text record:
Type Name Format: NFC Forum well-known type
Short Record
type: "T"
encoding: UTF-8
lang: "en"
text: "
START
10/06/2019 22:45
+20.60811 -103.4168
FINAL
10/06/2019 22:46
+20.60872 -103.4169
TIME
1.0 MIN
VEL
4.6365 Km/H
DIST
94.0196 M"
Payload length: 138 bytes
```

Figure 2-1 Travel complete message

The system peripherals are composed of the following modules, NFC reader and the main Electronic Control Unit (ECU) as the element A, the GPS antenna and module as element B that is connected through UART to the main ECU, and the LED matrix as the element C that is connected via SPI to the main ECU. these modules are shown in Fig. 2-2. The communication

between these 3 subcomponents was arbitrated through an RTOS that determined the order and the priority when running the communication tasks.

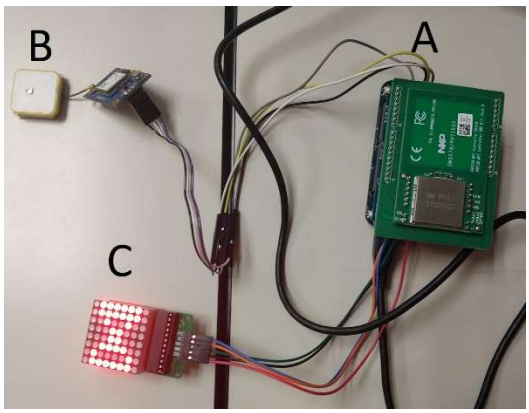


Figure. 2-2 Prototype *(A: MCU board and NFC board, B: GPS module with antenna, C: LED Matrix board)*

The LED matrix is connected to a display driver IC, which is connected to the main ECU via the SPI. On initialization, a picture of an hourglass is visible, indicating bad connection between the main ECU and GPS module. The LED Matrix is used as a Human Device Interface to show the user the state of the system also simulates the opening of the lock with the change between images of a closed and open lock as in Fig. 2-3.

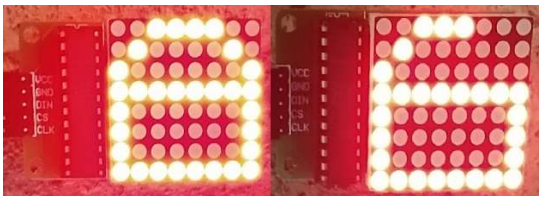

Figure 2-3 LED Matrix as HDI

# 3. Conclusion

In this paper we show the development of an embedded device that recollects data via different data sources. Furthermore, the device safeguards the information and transfers it via NFC to authorized users. As a security enhancement, an electromechanical lock was added to secure the vehicle against unauthorized users, and only unlocks when an authorized tag is presented.

The proposed solution focuses on cycling, however, the device can be easily adapted to other areas, such as the transportation sector, since it has applicability to recollect trip data like total distance traveled, location, start position, end position, and average speed, among others. For future work, the prototype can be improved into a final presentable product for public or private use. Another improvement is the user interface, as currently the device only offers basic configuration commands.

# 4. References


[1] «What Is NFC? | NFC Forum,» 15 july 2019. [En línea]. Available: https://nfc-forum.org/what-is-nfc/. [Último acceso: 15 july 2019].

[2] «What It Does | NFC Forum,» 15 july 2019. [En línea]. Available: https://nfc-forum.org/what-is-nfc/what-it-does/. [Último acceso: 15 july 2019].

[3] R. Steffen, J. Preißinger, T. Schöllermann, A. Müller y I. Schnabel, «Near Field Communication (NFC) in an Automotive Environment,» de *2010 Second International Workshop on Near Field Communication*, 2010.

[4] M. Pasquet, J. Reynaud y C. Rosenberger, «Secure payment with NFC mobile phone in the SmartTouch project,» de *2008 International Symposium on Collaborative Technologies and Systems*, 2008.

[5] H. Kato, Y. Sakajyo y S. Kaneda, «Visualization Method for Bicycle Rider Behavior Analysis Using a Smartphone,» de *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2017.

[6] Yizhai Zhang, Kuo Chen y Jingang Yi, «Dynamic rider/bicycle pose estimation with force/IMU measurements,» de *2013 American Control Conference*, 2013.

[7] X. Lu, K. Yu, Y. Zhang, J. Yi y J. Liu, «Whole-body pose estimation in physical rider-bicycle interactions with a monocular camera and a set of wearable gyroscopes,» de *2014 IEEE/RSJ International Conference on Intelligent Robots and Systems*, 2014.

[8] W. A. Hufstetler, M. J. H. Ramos y S. Wang, «NFC Unlock: Secure Two-Factor Computer Authentication Using NFC,» de *2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2017.

[9] R. L. Jorda, J. R. A. Coballes, L. A. C. Enriquez, M. L. S. Millan, A. J. Mora, M. N. G. Teodoro, N. M. Arago, A. C. Thio-ac y L. K. S. Tolentino, «Comparative Evaluation of NFC Tags for the NFC-Controlled Door Lock with Automated Circuit Breaker,» de *2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology,Communication and Control, Environment and Management (HNICEM)*, 2018.

[10] C. Daniela-Iulia y P. Sever, «Presentation of Several Secure Access Systems and Implementations,» de *2019 11th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, 2019.

[11] «NFC Forum Technical Specifications | NFC Forum,» [En línea]. Available: https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/nfc-forum-technical-specifications/.

[12] T. Monawar, S. B. Mahmud y A. Hira, «Anti-theft vehicle tracking and regaining system with automatic police notifying using Haversine formula,» de *2017 4th International Conference on Advances in Electrical Engineering (ICAEE)*, 2017.

[13] N. A. Chattha, «NFC — Vulnerabilities and defense,» de *2014 Conference on Information Assurance and Cyber Security (CIACS)*, 2014.